FRAUD AND INTERNAL CONTROLS WORKSHOP

ASMC PDI 2001
Dallas, Texas

Jim Cornell
Ed Romesburg

Defense Finance and Accounting Service

Your Financial Partner @ Work

Overview

- Internal Controls
- What is Fraud?
- Cyberthreats
- Red Flags
- What Can Be Done
- DFAS Initiatives
- Summary

Internal Controls Defined

- Internal controls are an integral component of an organization's management, providing reasonable assurance that agency objectives are being achieved.
- Critical "checks and balances" against:
  - Mission Failure
  - Fraud, Waste and Abuse
- Serve as the first line of defense to prevent and detect fraud

Aspects of an Internal Control Program

- A continuous built-in component of operations
- A series of actions and activities occurring throughout operations on an ongoing basis
- Effected by people
- Provides reasonable, not absolute, assurance that assets and resources are being safeguarded

Why Do We Need Controls?

- Ensure mission accomplishment
- Reduce opportunity for fraud
- Prevent loss of funds or other resources
- Establish standards of performance
- Assure compliance
- Preserve integrity
- Eliminate adverse publicity and public confidence

Consequences of Weak Internal Controls

- Waste - extravagant, careless, or needless expenditure of funds or the consumption of property resulting from deficient practices, systems, controls, or decisions

- Abuse - furnishing excessive services to beneficiaries; violating program regulations; and performing improper practices

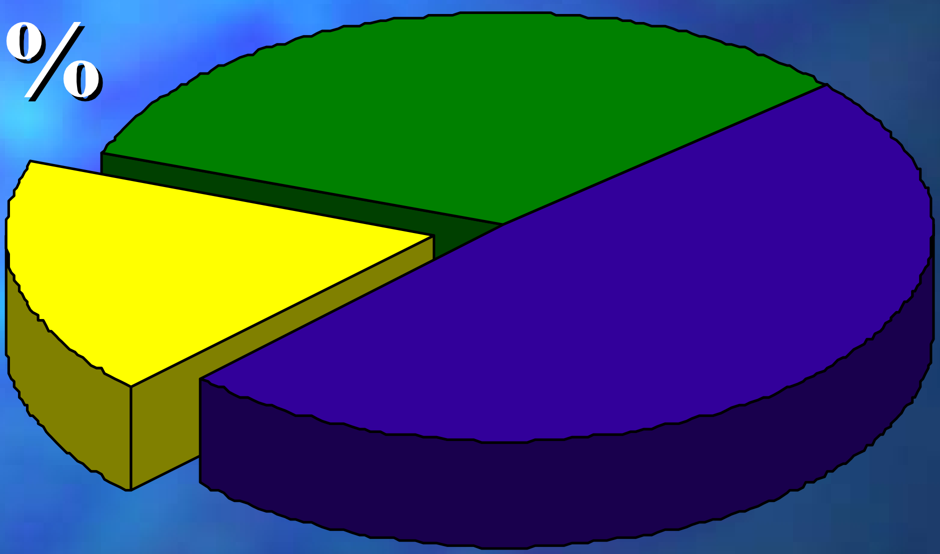
- Mismanagement - covers acts of waste and abuse; also, abuse of authority

Consequences of Weak Internal Controls

Fraud - a deliberate deception perpetrated for unlawful or unfair gain.

A *representation*
about a *material* point
that is *false*
that is *intentional or reckless*
that is *believed*
that is *acted upon* by the victim
wherein the victim suffers *loss*

How Fraud Is Detected



Source: Association of Certified Fraud Examiners

Conditions Fostering Fraud

- Fraudulent activity generally occurs when:
  - A pressure or incentive exists to commit fraud
  - There is a perceived opportunity to commit fraud

Why We Are Susceptible to Fraud

Organizations feel the pressure:

- **Get work done on time**
- **Minimize backlog**
- **Reduce interest payments**
- **Be responsive to customer**
- **Reduce the cost of operations**

Why We Are Susceptible to Fraud

- Inconsistent Application of Controls:
  - Trust rather than control
  - Organizational changes
- Unethical/Illegal behavior results from:
  - Little or no recognition of achievements
  - Personal financial worries/greed

Current DoD Environment

- Functional areas engaged in simultaneous reform
- Coordination and integration of hundreds of reform initiatives
- Increased vulnerability to waste, fraud, mismanagement
- DoD can best mitigate increased risk with improved, not eliminated, internal controls

Organizational Losses

- $9.00 per day per employee
- $400 billion annually

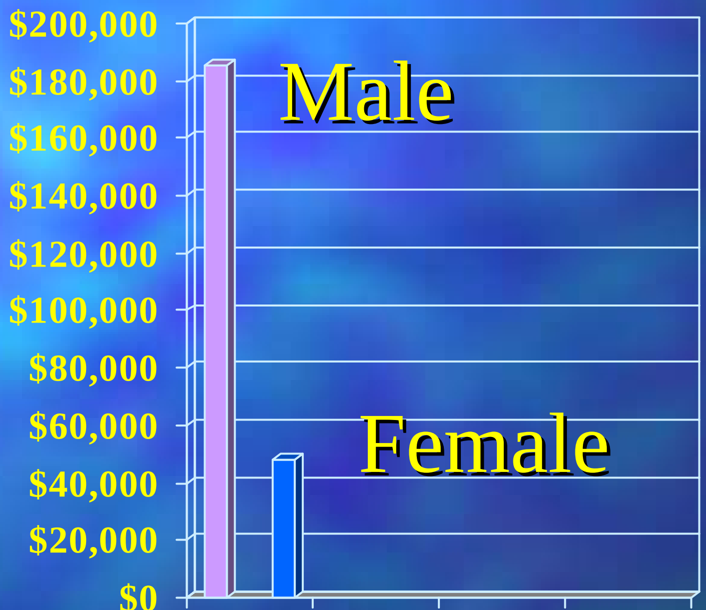
Source: Association of Certified Fraud Examiners

Who Commits Fraud?

Trusted management, employees, and suppliers who have access to data and resources.

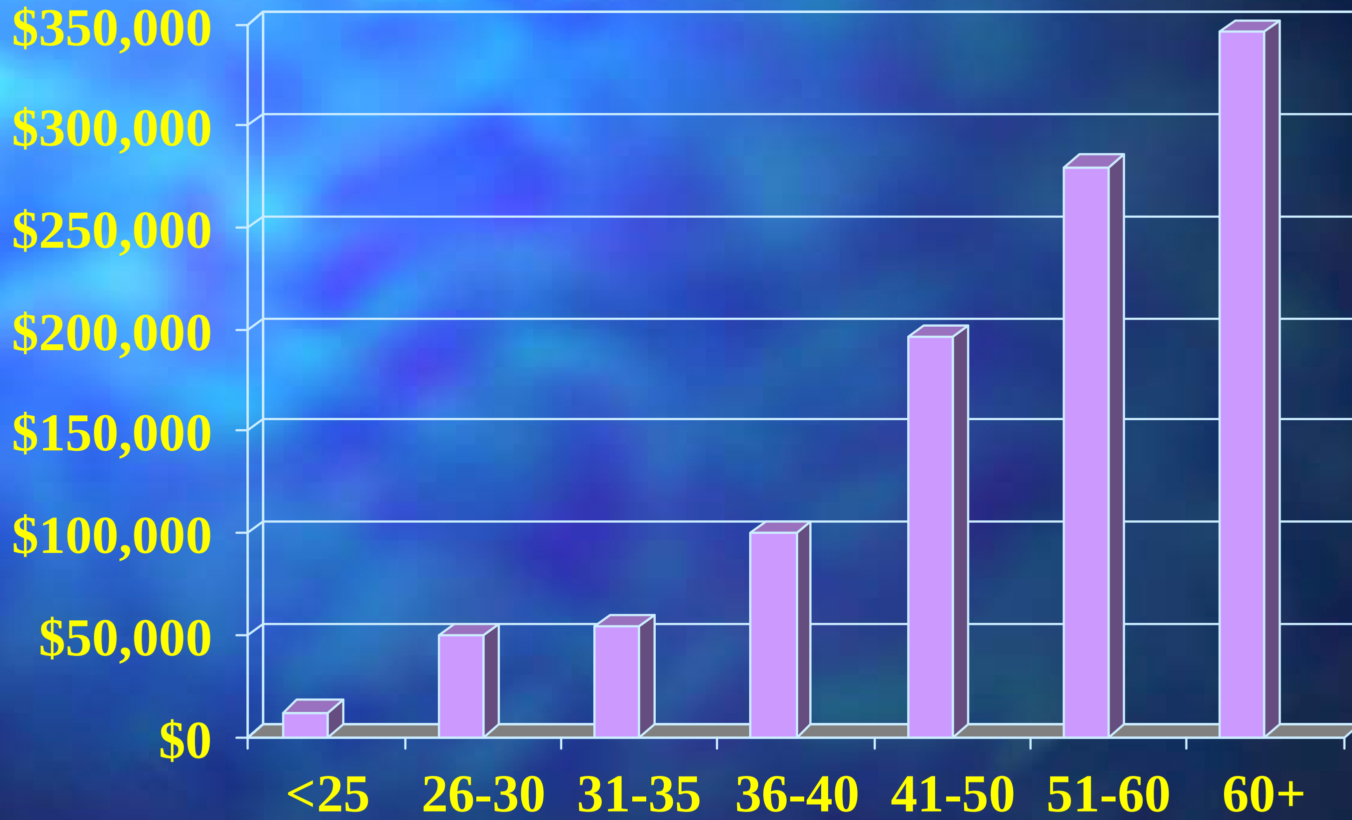
Source: Association of Certified Fraud Examiners

Median Individual Loss by Gender



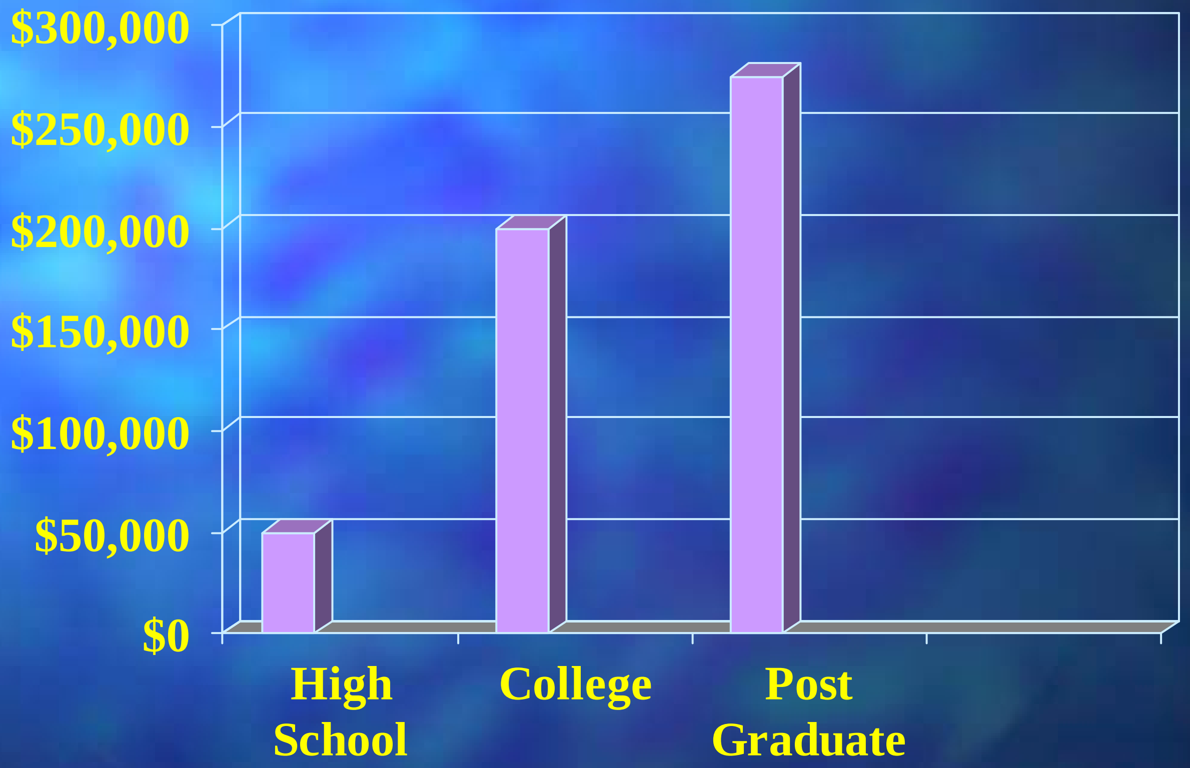
Source: Association of Certified Fraud Examiners

Median Individual Loss by Age



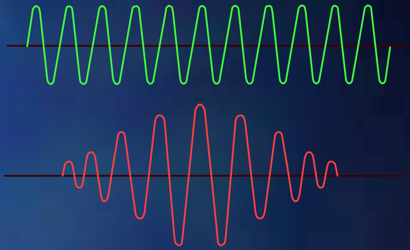
Source: Association of Certified Fraud Examiners

Median Loss by Educational Levels



Source: Association of Certified Fraud Examiners

CyberThreat



What is it?

Any illegal act for which knowledge of computer technology is used to commit a crime

Source: Association of Certified Fraud Examiners

Intrusion

The hacker "breaks" into the computer with "root" level privileges

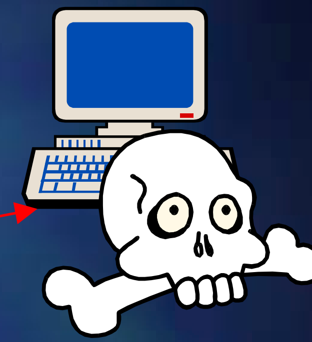
The criminal breaks into and steals your valuables

Source: Defense Criminal Investigative Services

CAT 2

Web Page Hack

The hacker defaces the Web Page



The vandal throws paint on the house

Source: Defense Criminal Investigative Services

CAT 3

ATTEMPT

The hacker attempts to access the computer, but is not successful

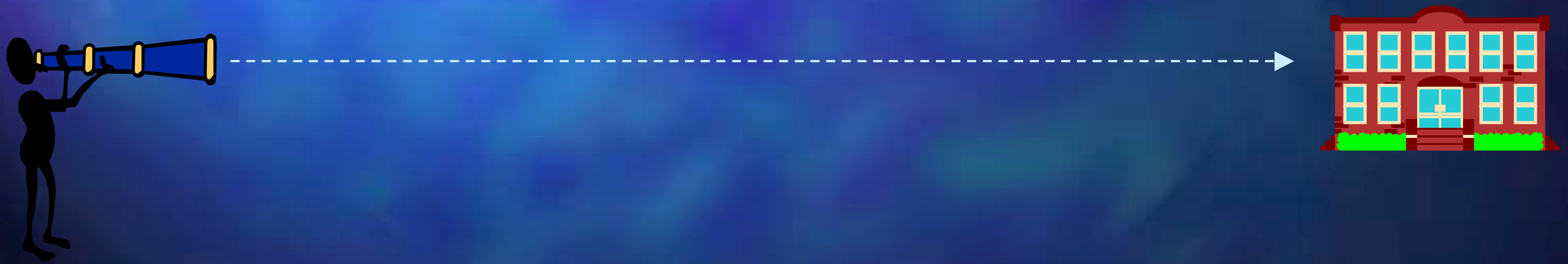
The fence (firewall/or other security measures) keeps the hacker out

Source: Defense Criminal Investigative Services

SCANNING

That network has 50 computers using port 24

That building has 10 windows and 1 door



Source: Defense Criminal Investigative Services

CAT 5

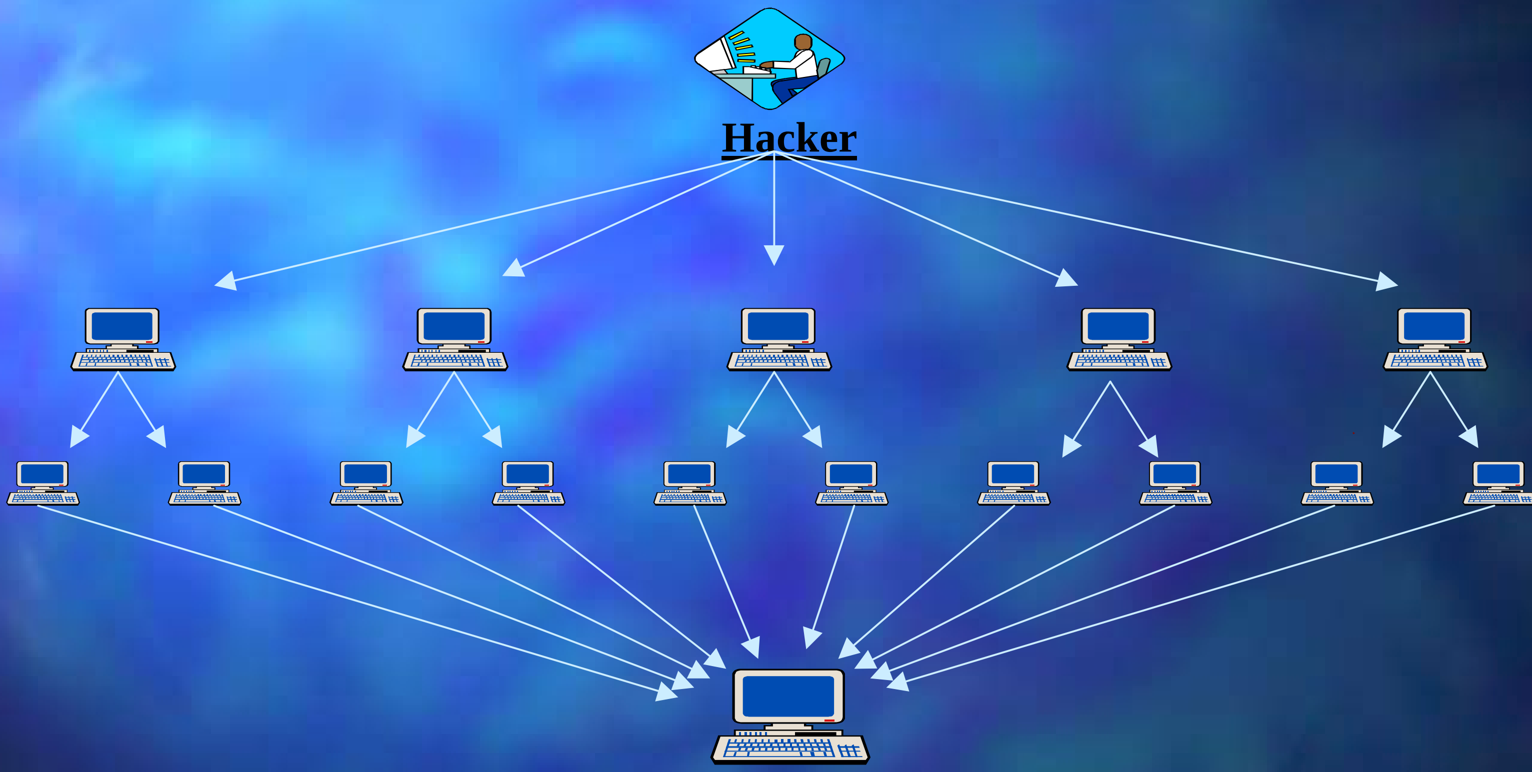
PROBING

That computer is using a version of unix that has a vulnerability at port 1524

The windows in that house are unlocked

Source: Defense Criminal Investigative Services

Trin00/DDOS



Source: *Association of Certified Fraud Examiners*

Email/Virus

CAT 7

Melissa/I Luv U

Source: Defense Criminal Investigative Services

Red Flags

Initial warnings that show a need for further review

Three Categories of Red Flags

- **Situational:**
  - high personal debt
  - perceived inequities
  - greed
  - urgent need for favorable performance
  - excessive use of alcohol or drugs
  - undue family/community expectations

Three Categories of Red Flags

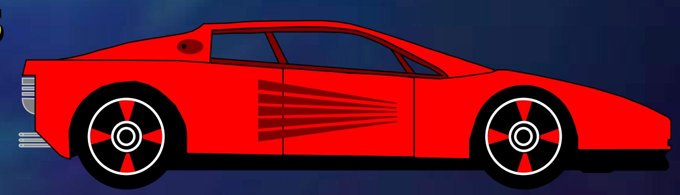
- **Opportunity:**
  - poor internal controls or accounting records
  - familiarity with operations
  - position of trust
  - close association with suppliers/key people
  - rapid turnover
  - inadequate training
  - dishonest management

Three Categories of Red Flags

- **Personal Characteristics:**
  - lack of morals
  - rationalizes contradictory behavior
  - poor credit rating or financial status
  - lack of stability

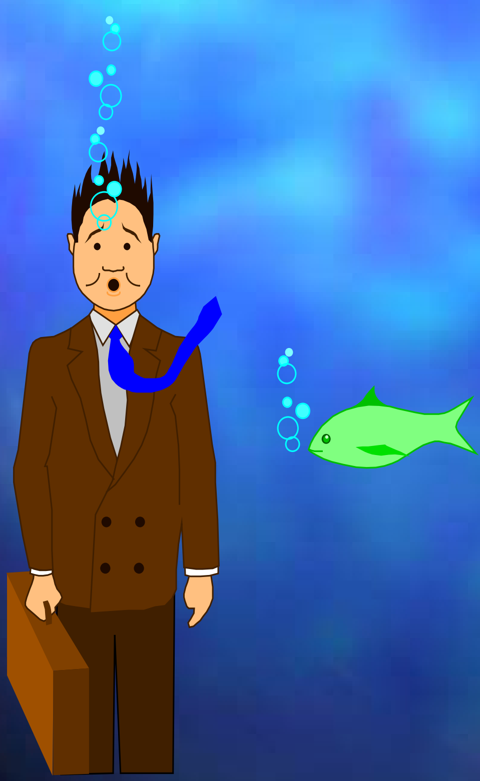
Warning Signs to Management

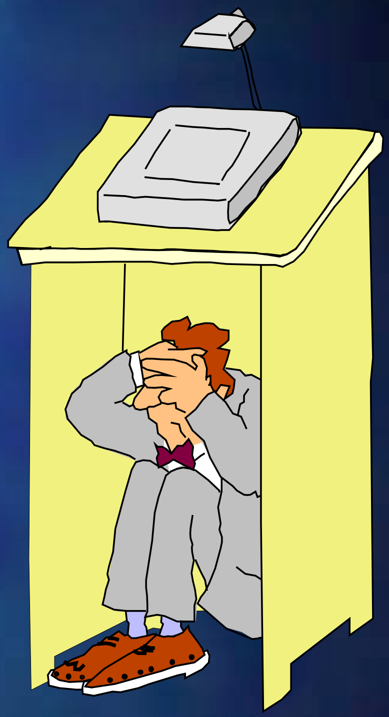
- Employee Lifestyle Improvements:
  - Expensive Cars
  - Extravagant Vacations
  - Expensive Clothing
  - New or Remodeled Homes
  - Expensive Recreational Property
  - Outside Investments



Warning Signs to Management

Behavioral Changes





What Can Be Done?

- Establishing:
  - Risk Assessment programs
- Strengthening:
  - Applications of internal controls
  - Fraud awareness
  - Ethics training
  - Internal Review Program
  - Penalties

Pro-Active Fraud Policies

- Comes from the Top
  - Senior Management Must Aggressively Seek Out Possible Fraudulent Conduct Instead of Waiting for Instances to Come to Their Attention

Management Responsibility Relating to Fraud

- Management should:

  - Understand the risk of fraud within the agency
  - Have knowledge of any fraud that has occurred within or against the agency
  - Have procedures in place to address risks

How DFAS is Responding To Fraud

- Established a separate Internal Review (IR) Directorate which reports directly to the Director of DFAS
- Established partnerships with:
  - Defense Criminal Investigative Service
  - Department of Defense Inspector General
  - Defense Manpower Data Center
  - Air Force Audit Agency
- Full integration of former Operation Mongoose into IR
- Educating the workforce: Develop and present fraud awareness briefings to all employees

How DFAS is Responding to Fraud (continued)

- Strengthening business process & operational review programs
- Requiring Internal Management Control Reviews [Federal Managers Financial Integrity Act (FMFIA)]
- Rating managers on actions to maintain or improve internal controls
- Strengthening system controls and firewall security

Electronic Business Fraud Vulnerability Assessment Group

- Sponsored by the Defense Criminal Investigative Service
- Current environment is to implement and utilize electronic business processes
- Group allows Defense Agencies to work together to protect electronic business processes against vulnerabilities to fraud

Interagency Fraud Work Group

- Sponsored by the Air Force Audit Agency
- Short-term Goal - Broader awareness of efforts within DoD to deter/detect financial fraud
- Long-term Goal - Establish partnership with other DoD agencies to address all aspects of combating financial fraud

Internal Review Seaside

- Detect and minimize fraudulent attacks against DoD financial assets
- Analyze cause of error or fraud to identify weaknesses in business processes
- Use enhanced technology
  - Data Mining
- Respond to Ad Hoc requests

Summary

Fraud is an organization's most formidable challenge today; it should not be accepted as just another cost of doing business.

Source: Association of Certified Fraud Examiners

To Report Fraud:

DoD Hotline 1-800-424-9098